

1. Introduction

Byron Bros is a large company known for making and selling products used for Personal Protective Equipment (PPE) industry. They have a large customer base and a significant supplier base as they import from and export to Europe and have a robust domestic market. Having all the data digits is bound to bring up issues. A plan would need to be created to guide Byron Bros to an era where they would conform to all the data protection laws.

2. Law, Policies & Ethics

To understand the issues Byron Bros will be facing, we first need to understand the definition of a law, policies, and ethics. Laws are rules set by the governing power that is acted or enforced; the rules will typically affect society members. The purpose of the law is to maintaining order, justice, peace in the society; this will then protect the general public and safeguard their interest. However, if any of the laws are violated, it will result in punishment or penalty for the offender. [1] Policies are instructions for a plan of action; they help guide users in achieving a particular set of goals. [2] A policy is a plan that the government aims to achieve for its citizens and society. Unlike laws, policies do not take a long time to change as they can be improved upon, and later if the legislation for the policies is passed, it will become a law. [3] Ethics is the philosophical part of our mind that guides the souls on what is good or bad; ethics is a critical concept in any human life, as it helps us make decisions regarding what is right or wrong. It informs us about how to act in a particular circumstance and make a judgment of our choices. [1]

2.1. Issues

As Byron Bros, a British based company, they will have to follow the laws of the land; some of these laws are the UK Data Protection Act 1998, Freedom of Information Act 2000, The Human Rights

Act 1998 (HRA) and the Computer Misuse Act 1990. these laws were put in place to help and safeguard the business. The company will also face issues with privacy, digital ownership, data gathering, accessibility, and maybe identity theft of the information they collect and store. Byron Bros may also be a victim of hiding crime, as not report such actions will keep their public image and clients satisfied; on the other hand, if such activities were to be informed, Byron Bros investors and clients may lose confidence. As Byron Bros growth will become higher, insider trading will become a concern for the company.

2.2. Legal Issues

Byron Bros will be facing the first legal issues: who will have access to their customer and supplier's personal data, and how will the data be protected, as this will need to be answered to follow the Data Protection Act 1998, how to prevent the unauthorised access to a computer system, as this will need to be answered to follow the Computer Misuse Act 1990.

2.3. Ethical Issues

In IT terms, privacy is a form that the consumer has freedom from observation; however, it is no more than a state of being free from unsanctioned intrusion. Customer data is some of the most valuable assets a company can obtain, and having a robust privacy system is essential. [4] Giving customers data privacy is critical; however, it is the methods by which the data is being gathered. National Security Agency (NSA) was given the authorisation to actively monitor citizens in the name of national security in the USA, as legislation or law was passed. [5] Accessibility of information is another issue with information security that Byron Bros will have to face. The right of a citizen or organisation to receive personal or

technical knowledge about others is known as accessibility. Nonetheless, these protections are occasionally ignored and exploited. [6]

2.4. Professional Issues

Insider trading is a method used by companies to obtain information about a rival company; the way the technique is used is that employers will be paid to leak information about the rival company or the general public. It is a common occurrence that high-level companies are a target for hackers, and occasionally the hackers will breach the security infrastructure of a company. However, the company has two options when this situation arises; they could either report the crime or do nothing. Reporting the crime would put their security infrastructure in question and give the company bad press while not reporting it will not affect the company's image in the short run; even if the hackers are discovered, most companies still would not report the crime.

2.5. Plan to Secure Data

There are numerous methods on how Byron Bros could protect their data; a few ideas I had were to have all staff members of the company be trained on how to use the systems that are put in place; this will reduce the likelihood that anything minor happens to the systems as staff members will have been drilled on what to do if the problem occurs. To ensure that only authorised members are signing into Byron Bros database and systems, a multi-factor authentication (MFA) will have to be implemented. This will make sure that only members of staff and workers will have access to Byron Bros systems. Implementing a strict permissions policy is another way that data can be protected. In any company, there will be members of staff that are higher ranking, for example, a network technician would have a lot more permissions than a member of staff from the sales department, by only showing each department data that is relevant to their department we are

eliminating any chances that an unauthorised person will gain access to data that they should not. [7] Most if not all of Byron Bros data will be stored in a data centre or on cloud storage systems; encrypting the data will make it difficult for anyone to read any information unless they have the encryption key; the encryption key should only be given to as few people as possible. Achieving a data recovery plan is another way to protect data. There must be backup made once or twice a week to have data to recovery as this ensures the minimal amount of downtime.

3. Roles and responsibilities

3.1. DPO

The GDPR law was introduced by the European parliament as a way to strengthen and streamline data protection for everyday European citizens. The law states that it is mandatory to appoint a data protection officer (DPO) at every organisation that processes or stores personal data for EU citizens as Byron Bros is a British based company, the law will apply to them. The primary role of a data protection officer is to educate company employees on how to manage the data that is stored, to train staff in data processing, which is mainly documenting and the collection of the data to make sure no mistakes are occurring, the DPO will also conduct reviews on company employees to make sure they understand the current data protection laws and will answer any questions we employees have about the data protection, create and a comprehensive report about all the data processing and activities that the company do which will then be given to the GDPR Supervisory Authorities. [8]

3.2. Information Security Engineers

An information security engineer's roles in a company or workplace are to enforce the information security plans and policies, ensuring that all staff members are following the laws set in place is paramount for the company. They will also be tasked with implementing new and quick ways to respond and recover from a security breach while also training new employees and staff members on the information security standards, policies and best practices. The installation and use of software will have to be chosen and installed by the information security engineer, software like the firewall, data encryption and VPN. Monitor the networks and systems for a potential security breach by using software that detects intrusions. [9]

3.3. IT security manager

Having an IT security manager in the company is an essential role as they can be used to achieve a number of tasks such as monitoring all operations and infrastructure; this is an important task as all the alerts and logs of the company's digital security footprint will be given to the IT security manager, and they would have to sift through the logs and respond to all the alerts, they would also have to monitor internal and external policy compliance, to make sure that members of staff understand the cybersecurity risk management policies and how to operate within that framework. The IT security manager will also be work with different departments in the organisation to reduce the risk of a data breach or any incident that will reflect negative on the company and make sure that all departments fully understand what they are doing. Performing audits is another task that will have to be done, regularly auditing the policies and procedures that were put into place. The audits will show if anything needs to improve or changes with any of the policies. [10]

4. Suitable Policies

4.1. Encryption policies

Having encryption policies will ensure that all data being sent and received will be encrypted. This will also apply to data stored on the companies database; the only way to break encryption is to gain access to the encryption key, which will only be given to essential staff members, limiting the number of people who have access to the key. The reason this policy was chosen is because of the General Data Protection Regulation (GDPR); the GDPR is a law that makes sure that data/information is [11] "used fairly, lawfully and transparently used for specified, explicit purposes used in a way

that is adequate, relevant and limited to only what is necessary. Accurate and, where necessary, kept up to date. Kept for no longer than is necessary. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage." [12]

4.2. Password policies

Password policies allow for greater security for passwords. It is a common occurrence that most people use the same password for most of their logins; however, the policy that will be introduced will require that a password will need to be changed every three months, the password would need a combination of letters, numbers and special characters, this will make it harder for unauthorised users to gain access into the systems and would advise that the passwords should not be written on a post-it note on the desk next to the user system.

4.3. Email policies

Email policies will resist the number of spam and viruses sent to an employee's email, as adequately trained employees would be able to spot the difference by encrypting personal emails and attachments; only the sender and recipient will see the information that was sent. Employees should use the company's email to speak formally. Any non-work related email should not be transmitted, as this reduces the chance of a phishing email being taken seriously. All emails will be monitored for any potential spam or phishing email.

5. Risk Management Framework

Risk management is a process of identifying potential risks to a company network, data or infrastructure; these risks could occur from a wide range of factors. Implementing a risk management framework can mitigate those potential risks, and it could act as a filter for any

potential risks. In the framework management created, the periodic reviews system will be used, as this is part of the risk management strategies as threats are constantly changing for a company. The first step is to identify the problem; for this example, the problem will be a data breach; identifying the problem can always be the most challenging part as many problems can go on undetected. The next step is to assess the damage is done, then find a solution to the problem, then the situation would be monitored, and a report will have to be created to illustrate the problem was and how to stop it from occurring later in the future. [13]

5.1. Risk Identification

There are many factors that come into consideration when trying to identify risks; in Byron Bros case, the main priority is their data stored. Some of these potential risks could be targeting the data stored. There are threats that could be potentially damaging to the company; this could be a form of intrusion, destruction or disclosure. A vulnerability is an opportunity for a threat to become a real issue or problem.

5.2. Risk Measurement

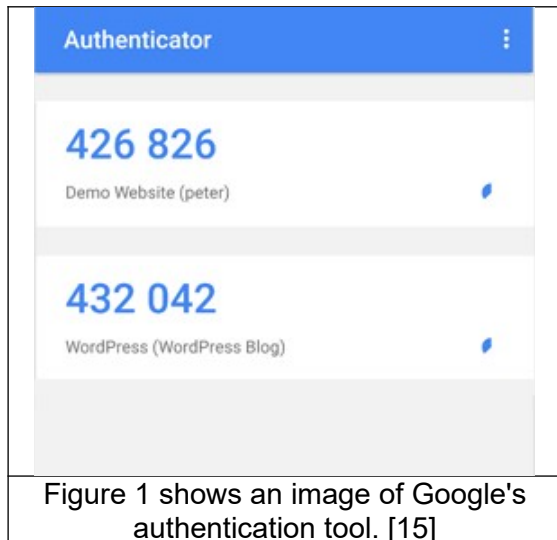
Once the risk has been identified, the company must first measure the security threat, the chances of the risk occurring, and the damages for risk will cause to the company.

5.3. Risk Mitigation

Once all the potential risk has been measured, the company will have a list of all the risks they are vulnerable to; this will then be put into a list that can then be organised from the highest threat to the lowest, however it would be impossible to try to mitigate all the potential risks, the company would then have to choose that risks below a certain level are not worth addressing because either because there is little probability of that threat to occur, or there are too many greater threats that needed to be attended to straight away and would fit into the company's work plan.

5.4. Monitoring

This stage of the process is critical, as monitoring the risks frequently will



significantly reduce the chances of the risk occurring again. It will be in the company's best interest to continuously monitor the risk in case of any further development.

5.5. Risk Reporting

After the potential risk has been identified, measured, mitigated and monitored, a report about the situation and how it was handled would need to be written; this will be a referencing point for later on in the future because if the risk occurs again, the company will have a report on how to deal with the problem. [14]

6. Implementation and maintenance

6.1. Access Controls

Access control is a method that computer systems use to figure out which users will gain access to their resources; there are three types of access control: mandatory access controls (MACs), discretionary access controls (DACs) Nondiscretionary controls. Access control has four fundamental functions: identifying the user, authenticate, authorise, and accountability; after all these steps, the end-user will gain access to the computer system resources. Identification is a

method that many organisations use to separate each user from each other, making them unique; this can be in department codes, random numbers, or special characters. Authentication is a method in which the user will need to prove that they are whom they say they are; this can be done using a password or an authentication tool, as shown in figure 1. Authorisation, once the user has, identifies themselves by using their authentication code, they will be granted access to the computer systems resources. To ensure that the account was not unlawfully accessed, so the computer systems would log that it has been signed into and that data will be saved, accountability is that the method is called.

6.2. Firewalls

Firewalls are a way to protect a network from potential attacks; there are different firewall methods used to protect data. The first method I will be talking about is filtering packets; the firewall uses this method to select which packets it wants to enter or leave the network; if a users IP address has been blacklisted, they will not be able to send packets from there IP address to the network that has there IP blacklisted because of the firewall. Another method that the firewall uses are application-layer proxy; application-layer proxy work by filtering out key terms or phrases from a search, this can be useful when the admin of the network would need to block specific words from showing up when a user searches for those terms. [16] Hybrids firewalls are a mix of all the other different types of firewalls. The next-generation Firewall (NGFW) is a combination of packet inspection with stateful inspection; it also uses deep packet inspection, malware filtering and antivirus. The NGFW is capable of tracking all traffic from Layer 2 to the application layer; this grants it more insight in filtering information.



Figure 2 showing the status of a Windows firewall

6.3. VPN

Virtual private networks (VPN) are network connections that allow the user to create their own private network, which provides the option for inter-connectivity and data to be transferred. The VPN that the user is connected to must first perform encapsulation which is a method of compressing a packet inside another packet. The packet will appear to the public as an ordinary packet; however, it is carrying private and sensitive data. The next step is the encryption of all data being sent and received. Allowing employees to use VPNs to gain access to their workstations when they are not there or working from home will be a good thing to implement.

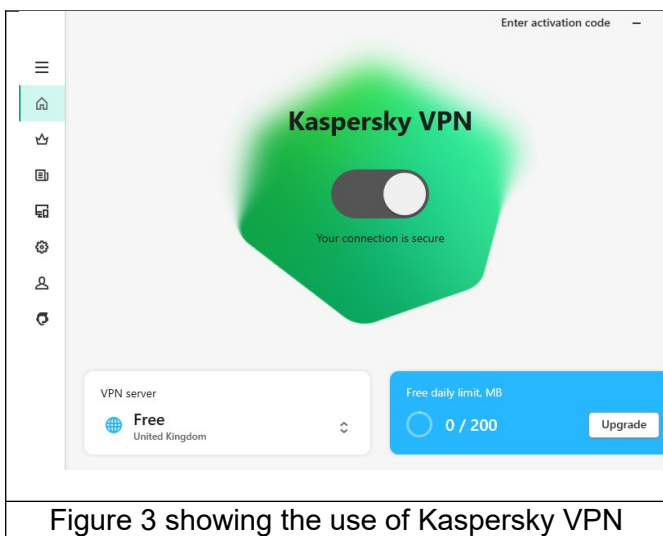


Figure 3 showing the use of Kaspersky VPN

6.4. Cryptography

Cryptography is a method of securing data by encrypting plain text into incomprehensible ciphertext, making it useless to a user who does not have the encryption key. The Cipher method is used in cryptography to encrypt plain text; this is done by each word being transformed at a time. This is called bitstream or the other method block cipher, which is when a message or data is divided into blocks that will then be encrypted one block at a time. Implementing cryptography into any company will make sure that only authorised users can see sensitive data.

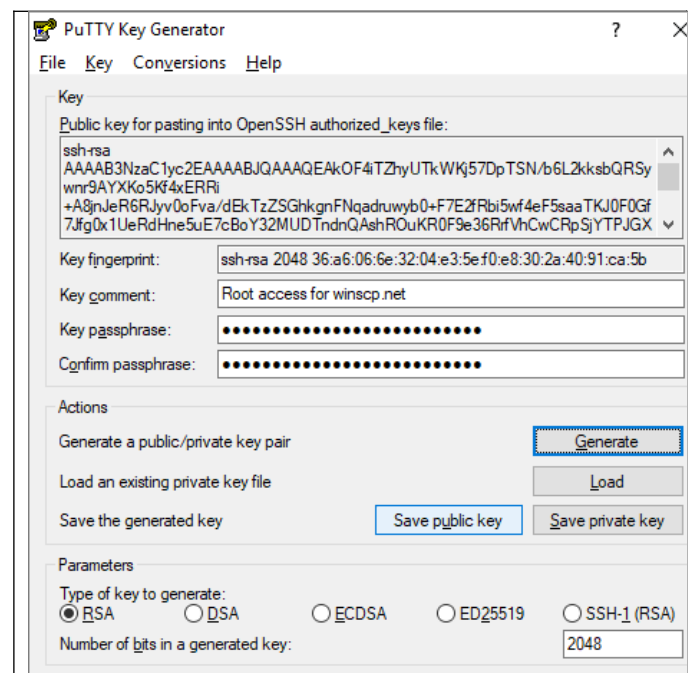


Figure 4 showing the use of a cryptography key generator

6.5. Physical Security

Physical security is the protection of physical items that the company obtains; these items need to be protected so unauthorised users will not gain access to them or cause damage to them. There are many ways to cause damage to physical damage to an item; for example, a server,

extreme heat or cold can cause damage also humid or dry air, liquids such as water, living organisms like viruses, bacteria, people, animals, insects and Movement like collapse, shearing, shaking, vibration, liquefaction, flow waves, these are some ways that could lead to the server getting damaged, so countermeasures will have to be put in place to maintain physical security, countermeasures such as walls, fencing, and gates this will keep out intruders from gaining access to the building, armed guards with dogs will also sojourn intrudes, the use of ID cards and badges makes sure authorised users gain entry into the building while locks and keys make sure that safes or doors will not be left open, in many banks a mantrap is used this is a room that only has one entry point and one exit point if a user wants to gain access into the building, but isn't authorised and they get denied the doors of the room will shut and the officers will be notified and the room would be with officers. Basic alarms and alarm systems are suitable for people to be notified when something occurs, like a fire alarm or a burglar alarm. The main priority for Byron Bros is to keep all their data safe; their data will most likely be stored in servers which are vulnerable to two things fire and a lack of electricity, so by implementing the Gaseous fire suppression system in case of a fire breaking out it is not likely that it will spread to any of the other buildings and with the use of a standby uninterruptible power supply (UPS) the server will never suffer from a power failure.

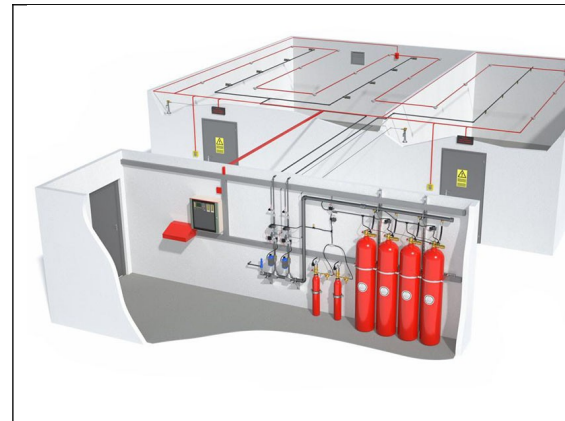


Figure 5 showing the layout of the Gaseous fire suppression system

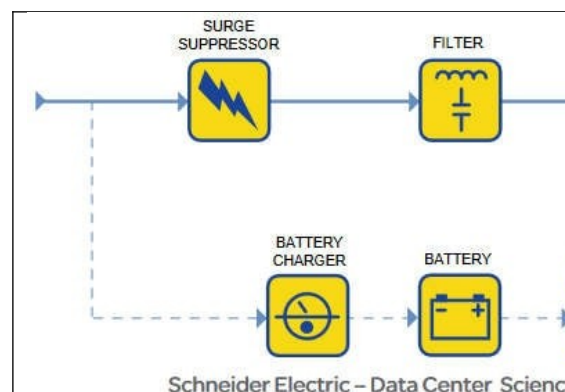


Figure 6 showing the standby uninterruptible power supply layout

7. Intrusion Detection System

The intrusion detection system that will be beneficial for the company is SolarWinds Security Event Manager. It provides an array of security features that will help protect the company and its data. Some of these features are user activity monitoring and access logging tool, which can be used to catch any suspicious logon and logoff attempts across any of the servers, workstations, and network devices, making it a lot difficult for any unauthorised users to gain access. As the event manager will be logging the logins and out, it will be able to identify anomalies. The intrusion detection system I chose can also automate compliance risk management, this is achieved by using a structured log, which was created to assist users in bettering their compliance risk assessment by enabling accelerated

validation of laws, restrictions, and internal policies implementation to locate weaknesses. The software is designed to identify any potential information security risk and policy breaches before they become critical issues.

Additionally, the software has built-in responses, then IT risk and compliance violations are detected. The software can help monitor the companies firewall by collecting logs of network traffic and events from the firewalls and IDS/IPS devices in realtime. As the software always gathers logs, the software can allow users to monitor any suspicious activity in realtime and proactively respond before threats develop. Phishing attacks are always hard to detect for most intrusion detection systems; however, SolarWinds Security Event Manager can identify, and a countermeasure can be deployed by using a tool call File Integrity Monitoring (FIM) which can be used to detect changes to files, folders, and registry settings, keeping any sensitive data safe. A spear-phishing attack is created to try and compromise login credentials; however, SolarWinds Security Event Manager is designed to recognise any noticeable shift in an account's usage pattern and send an alert to the necessary admin to find out what is going on with the account. The software also has builtin realtime monitoring of their network firewall; this allows the admin to identify any strange activities that occur, for example, an IP address is repeatedly asking for a requested that is humanly possible; besides, the admins have the option to work with software that has pre-configured rules or set customised ones so that they can perform effective intrusion detection. The software is also compatible with the Mac operating system and Linux so that it can be used in any scenario. With all these features, it shows that SolarWinds Security Event Manager is a robust system that would react against information security threats; however, the only negative side to using this software is

that it will need to be updated constantly, which will introduce a lot of downtime, apart from that it is an excellent system to implement in Byron Bros company.

8. Conclusion

Byron Bros, the small company that makes personal protective equipment that will transition from storing customers data in file cabinets to storing their data on a server; this will be made possible with a structured document/ plan by following and comply with the data protection laws and policies it will be possible for the company to start storing personal customer data; however, following laws and policies will not be enough, there needs to be an enforcer for the policies/laws so a DPO will have to be appointed, the DPO will also be taking audits of the company and will be tasked on coming up with new ideas for data protection. A risk Management Framework was created to determine any potential risks that the company might be in and how the company will deal with its issues. An intrusion detection system was also recommended in the document and would help guide the company to feather protecting its data; numerous systems will have to be put in place to protect the server, like gaseous fire suppression system and a UPS, just in case and if all goes well Byron Bros can be an operating company will no problems.

